AMENDMENTS TO THE CLAIMS

Please amend the claims as indicated below. This listing of the claims replaces all prior versions and listings of claims in this application.

1. (Currently Amended) A method of responding to an overload condition at a network element ("victim") in a set of one or more potential victims on a network, the method comprising the steps of:

A. responsively to an indication of an anomalous traffic condition, initiating diversion of traffic destined for the victim by a first set of one or more network elements external to the set of one or more potential victims to a second set of one or more network elements external to the set of one or more potential victims,

B. the element(s) of the second set filtering traffic diverted in step A ("diverted traffic") and selectively passing a portion thereof to the victim,

wherein said filtering step includes detecting any of (i) a traffic pattern that differs from an expected pattern and (ii) traffic volume that differs from an expected volume, said expected pattern and said expected volume being determined during a period in which the victim is not at an overload condition, and

wherein said detecting step includes determining whether any of the traffic pattern and volume varies statistically significantly from any of the expected pattern and volume, respectively.

2. (Previously presented) A method according to claim 1, wherein the initiating step includes effecting a path of traffic that differs from a path that traffic would otherwise take to the victim.

3. (Cancelled)

4. (Original) A method according to claim 1, wherein the filtering step includes detecting suspected malicious traffic.

5. (Original) A method according to claim 4, wherein the detecting step includes detecting packets with spoofed source addresses.

6. (Previously presented) A method according to claim 1, wherein the filtering step includes detecting traffic requiring a selected service from the victim.

7. (Original) A method according to claim 6, wherein the filtering step includes discarding traffic not requiring the selected service from the victim.

8. (Original) A method according to claim 7, wherein the filtering step includes discarding any of UDP and ICMP packet traffic.

9. (Cancelled)

10. (Previously presented) A method according to claim 1, comprising operating one or more elements of the first set at points on the network around the set of one or more potential victims.

11. (Original) A method according to claim 10, comprising operating one or more elements of the second set any of adjacent to or external to one or more elements of the first set.

12. (Cancelled)

13. (Previously Presented) A method according to claim 10, wherein the anomalous traffic condition is indicative of a distributed denial of service (DDoS) attack.

14. (Previously Presented) A method according to claim 10, comprising selectively activating the one or more elements of the first set by declaring a network address of the victim to be close in network distance to one or more elements of the second set.

15. (Previously Presented) A method according to claim 10, comprising associating the victim with first and second addresses, and wherein the filtering step includes

discarding traffic received external to an area defined by the points directed to the first address, and

passing to the victim traffic received external to an area directed to the second address.

16. (Original) A method according to claim 10, wherein the diverting step includes redirecting traffic using Policy Based Routing.

17-19. (Cancelled)

20. (Previously Presented) A method according to claim 5, wherein detecting the packets with spoofed source addresses comprises executing a verification protocol with sources of the diverted traffic, and wherein the passing step includes passing to the victim traffic from a source that correctly complies with the verification protocol.

21-32. (Cancelled)

33. (Previously Presented) A method according to claim 1, wherein the filtering step includes statistically measuring any of a traffic pattern and volume so as to identify any of a source and a type of the overload condition.

34. (Cancelled)

35. (Previously Presented) A method according to claim 33, comprising determining any of the traffic pattern and volume during a period when the victim is not in the overload condition, for comparison with any of the traffic pattern and volume in the filtering step upon detecting the anomalous traffic condition.

36-45. (Cancelled)

46. (Currently Amended) A network element for use in protecting against an overload condition on a network, the network element comprising:

an input for receiving traffic diverted from the network, the traffic comprising flows of data packets having respective source addresses;

a statistics module that is arranged to perform a statistical analysis of the diverted traffic so as to detect an anomalous pattern of a flow associated with at least one of the source addresses;

a filter, which is operative, responsively to detection of the anomalous pattern, to block at least a portion of the data packets having the at least one of the source addresses; and

an output coupled to the input for selectively passing on to further elements in the network traffic not blocked by the filter,

wherein said statistical analysis comprises detecting any of (i) a traffic pattern that differs from an expected pattern and (ii) traffic volume that differs from an expected volume, said expected pattern and said expected volume being determined during a period in which the victim is not at an overload condition, and determining whether any of the traffic pattern and volume varies statistically significantly from any of the expected pattern and volume, respectively.

47. (Original) A network element according to claim 46, comprising a termination detection module that at least participates in determining when the overload condition has ended.

48. (Previously Presented) A network element according to claim 46, comprising an antispoofing element that performs at least one of authenticating and verifying a source of traffic.

49. (Currently Amended) A system for use in protecting against an overload condition on a network, the system comprising:

one or more network elements ("guards") disposed on the network, each network element having

an input for receiving traffic from the network,

a filter coupled to the input, the filter selectively blocking traffic originating from a source suspected as potentially causing the overload condition,

a statistics module that is coupled to the filter and that identifies the traffic statistically indicative of having originated from the source suspected as potentially causing the overload condition, and

an output coupled to the input for selectively passing on to further elements in the network traffic not blocked by the filter,

one or more further network elements ("diverters") disposed on the network and in communication with the guards, the further network elements selectively initiating, responsively to detection of an anomalous traffic condition, diversion to at least one of the guards traffic otherwise destined for a still further network element ("victim") in a set of one or more potential victims on the network,

wherein said statistics module performs statistical analysis comprising detecting any of (i) a traffic pattern that differs from an expected pattern and (ii) traffic volume that differs from an expected volume, said expected pattern and said expected volume being determined during a period in which the victim is not at an overload condition, and determining whether any of the traffic pattern and volume varies statistically significantly from any of the expected pattern and volume, respectively.

50. (Previously Presented) A system according to claim 49, wherein at least one of the guards comprises a termination detection module that at least participates in determining when the overload condition has ended.

51. (Previously Presented) A system according to claim 49, wherein at least one of the guards comprises an ingress filter, coupled to the statistics module, that generates and transmits to a further network element on the network rules for blocking traffic on the network.

52. (Previously Presented) A system according to claim 49, comprising an antispoofing element that any of authenticates and verifies a source of traffic.

53. (Previously Presented) A method according to claim 1, wherein diverting the traffic comprises diverting all of the traffic destined for the victim upon detecting the anomalous traffic condition.

54. (Previously Presented) A method according to claim 1, and comprising learning an expected pattern of the traffic while the victim is not under attack, wherein detecting the anomalous traffic condition comprises determining that the traffic differs significantly from the expected pattern.

55. (Currently Amended) A method of responding to an overload condition at a network element ("victim") in a set of one or more potential victims on a network, the method comprising the steps of:

A. responsively to an indication of an anomalous traffic condition, initiating diversion of traffic destined for the victim by a first set of one or more network elements external to the set of one or more potential victims to a second set of one or more network elements external to the set of one or more potential victims,

B. the element(s) of the second set filtering traffic diverted in step A ("diverted traffic") and selectively passing a portion thereof to the victim,

wherein the initiating step includes effecting a path of traffic that differs from a path that traffic would otherwise take to the victim, ~~and~~

wherein the first set of one or more network elements comprises network switches having respective ports, comprising at least one switch that is configured to route the traffic to the victim through a first port while the victim is not under attach, and wherein effecting the path comprises instructing the at least one switch to route the traffic destined for the victim through a second port, to which at least one of the network elements in the second set is coupled,

wherein said filtering step includes detecting any of (i) a traffic pattern that differs from an expected pattern and (ii) traffic volume that differs from an expected volume, said expected pattern and said expected volume being determined during a period in which the victim is not at an overload condition, and

wherein said detecting step includes determining whether any of the traffic pattern and volume varies statistically significantly from any of the expected pattern and volume, respectively.

56. (Currently Amended) A method of responding to an overload condition at a network element ("victim") in a set of one or more potential victims on a network, the method comprising:

diverting to a guard machine traffic destined for the victim, the traffic comprising flows of data packets having respective source addresses;

performing a statistical analysis of the diverted traffic at the guard machine so as to detect an anomalous pattern of a flow associated with at least one of the source addresses; and

responsively to detecting the anomalous pattern, preventing at least a portion of the data packets having the at least one of the source addresses from reaching the victim while passing to the victim at least some of the data packets from other source addresses,

wherein said performing step includes learning an expected traffic pattern of the flows while said victim is not under attack and is not in an overload condition, and detecting an attack by determining that the anomalous pattern differs statistically significantly from the expected traffic pattern.

57. (Cancelled)

58. (Previously presented) A method according to claim 56, wherein performing the statistical analysis comprises detecting any of a traffic volume, port number distribution, periodicity of requests, packet properties, IP geography, and distribution of packet arrival/size.

59. (Previously presented) A method according to claim 56, and comprising processing the diverted traffic so as to detect and discard the data packets that have one or more spoofed source addresses before performing the statistical analysis.

60. (Previously presented) A method according to claim 59, wherein processing the diverted traffic comprises initiating a protocol handshake between the guard machine one or more of the source addresses in order to determine that the one or more of the source addresses are spoofed.

61. (Previously presented) A method according to claim 56, wherein preventing at least the portion of the data packets comprises filtering out the diverted packets that have the at least one of the source addresses.

62. (Previously presented) A method according to claim 61, wherein filtering out the diverted packets comprises discarding the diverted packets that have the at least one of the source addresses before performing the statistical analysis on the diverted traffic that remains after the discarding.

63. (Previously presented) A method according to claim 62, and comprising processing the diverted traffic after discarding the diverted packets that have the at least one of the source addresses so as to detect and discard the data packets that have one or more spoofed source addresses before performing the statistical analysis.

64. (Previously presented) A method according to claim 56, wherein performing the statistical analysis comprises at least one of analyzing one or more of netflow data, server logs, victim traffic, and traffic volume, and classifying the statistical analysis according to types of users that generated the traffic.

65. (Previously presented) A method according to claim 56, wherein performing the statistical analysis comprises classifying the traffic according to types of users that generated it.

66. (Currently amended) A method of responding to an overload condition at a network element ("victim") in a set of one or more potential victims on a network, the method comprising:

coupling the victim to receive traffic from the network via a first port of a network switch;

actuating the network switch to divert the traffic destined for the victim to a second port to which a guard machine is coupled;

filtering the diverted traffic using the guard machine; and

selectively passing at least a portion of the filtered traffic from the guard machine to the victim,

wherein said filtering comprises performing statistical analysis comprising detecting any of (i) a traffic pattern that differs from an expected pattern and (ii) traffic volume that differs from an expected volume, said expected pattern and said expected volume being determined during a period in which the victim is not at an overload condition, and determining whether any of the traffic pattern and volume varies statistically significantly from any of the expected pattern and volume, respectively..

67. (Previously presented) A method according to claim 66, wherein the network switch comprises a router.

68. (Previously presented) A method according to claim 66, wherein selectively passing at least the portion of the filtered traffic comprises passing the filtered traffic from the guard machine to the network switch, for transmission to the victim via the first port.

69. (Previously Presented) A method according to claim 66, wherein filtering the diverted traffic comprises performing a statistical analysis of the diverted traffic so as to detect an anomalous pattern of a flow associated with at least one source address of the traffic, and responsively to detecting the anomalous pattern, preventing at least a portion of the data packets having the at least one source address from reaching the victim